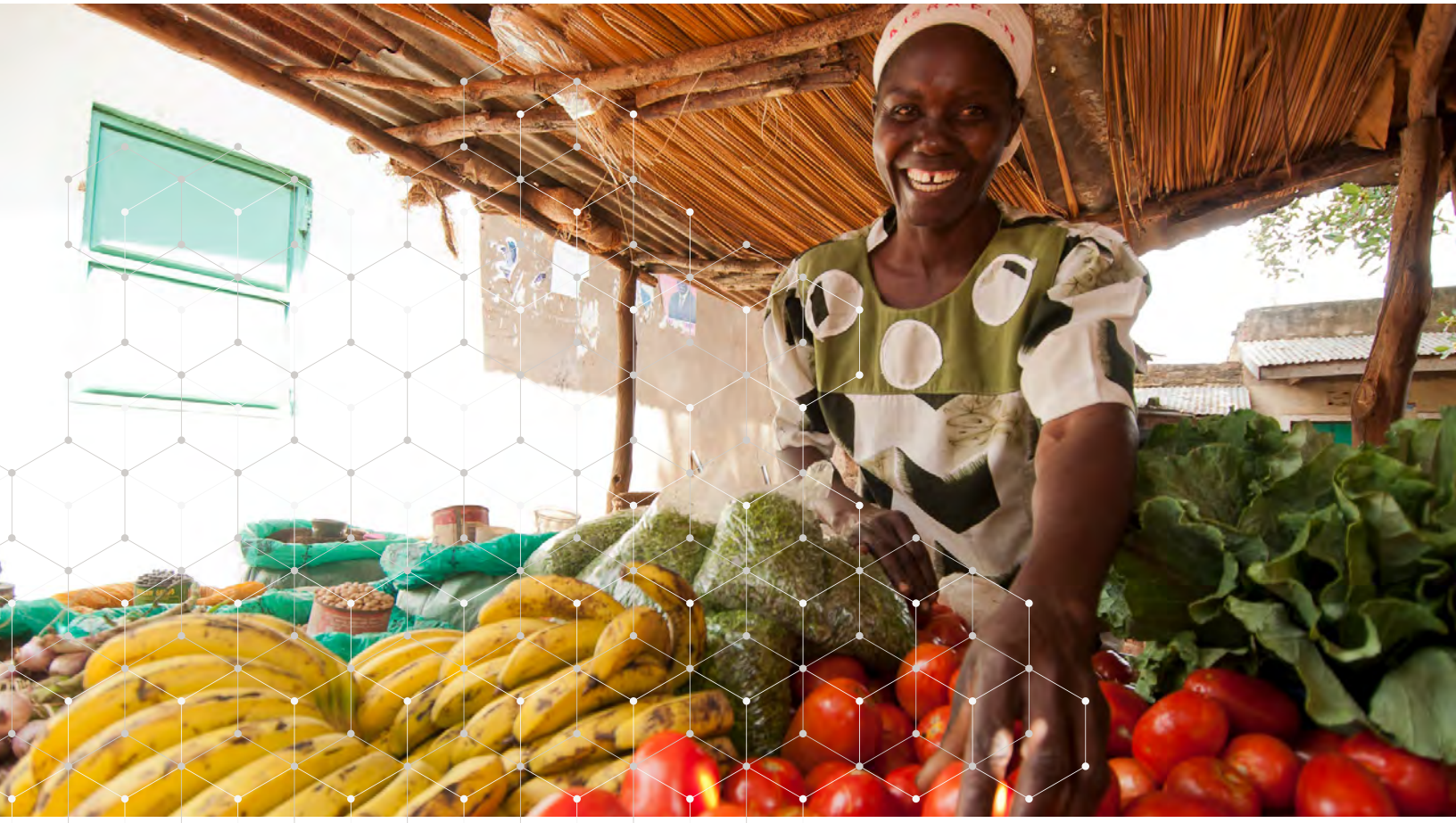
USAID
FROM THE AMERICAN PEOPLE

Guía de Ciberseguridad para Pequeñas y Medianas Empresas



PARTE 2:
PROTEGIENDO SU EMPRESA

RECONOCIMIENTOS

La Guía de Ciberseguridad para Pequeñas y Medianas Empresas fue desarrollada con la asesoría de la Agencia de Desarrollo Internacional de los Estados Unidos (USAID, por sus siglas en inglés), de la Oficina para el Desarrollo, Democracia e Innovación (DDI, por sus siglas en inglés), por el Centro para el Desarrollo Económico y de Mercado (EMD, por sus siglas en inglés) y redactado principalmente por Daniel Vázquez en el marco de la Actividad de Comercio y Competitividad implementada por Resonance Global. Las contribuciones y revisiones adicionales fueron proporcionadas por Clare Sullivan del Centro de Investigación Cyber SMART de la Universidad de Georgetown, así como por Jeremy Ravenelle, Evan Legé y Anne Szender McCarthy de la Actividad de Comercio y Competitividad.

Este documento fue elaborado para su revisión por la Agencia para el Desarrollo Internacional de los Estados Unidos. Asimismo, fue preparado por la Actividad de Comercio y Competitividad, con el número de contrato AID-OAA-C-17-00110. Su contenido es responsabilidad exclusiva del autor y no refleja necesariamente las opiniones de USAID o las del Gobierno de los Estados Unidos.

TABLA DE CONTENIDOS

Glosario de Términos 2

Lista de Acrónimos 3

Introducción 5

La Importancia de un Buen Líder 5

Dónde empezar 7

1. Capacitar a los empleados a confiar, pero verificar 7
2. Instalar un software antivirus y antimalware confiable 8
3. Usar cortafuegos de web 8
4. Elegir contraseñas seguras 9
5. Utilizar la autenticación multifactor 10
6. Actualizar el software de manera regular 10
7. Cifrar todos los datos confidenciales 10
8. Asegurar las conexiones Wi-Fi 10
9. Supervisar los sistemas de pago 12
10. Mantener el sitio web de la empresa seguro 12
11. Evitar que los teléfonos móviles sean objetivos de ataqu 14
12. Mantener copias de seguridad de toda la información 15
13. Recordar que la seguridad física es parte de la ciberseguridad 17
14. Explorar la posibilidad de un seguro cibernético 17
15. Considerar contratar a un profesional de TI 19

Si Ocurre un Incidente de Ciberseguridad 21

Reanudar Operaciones 21

Gestionar las Comunicaciones de forma efectiva 21

Notificar a las Autoridades 22

Notificar a los Proveedores de Servicios 23

Notificar a los Clientes 24

Medios Sociales 24

Aprendiendo del Incidente 25

Conclusión 26

GLOSARIO DE TÉRMINOS

Software antivirus: programa que monitorea una computadora o red para detectar o identificar los principales tipos de código malicioso y prevenir o contener incidentes de malware, en ocasiones eliminando o neutralizando el código malicioso.[1]

Criptomoneda: una moneda digital en la que las transacciones se verifican y los registros se mantienen mediante un sistema descentralizado que utiliza criptografía en lugar de una autoridad centralizada. Algunos ejemplos son Bitcoin, Ethereum, Monero, etc.

Ataque cibernético: ataque por el ciberespacio cuyo objetivo es el uso del ciberespacio por parte de una organización, con el fin de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura informática o destruir la integridad de los datos o robar información controlada.[3]

Ciberseguridad: actividad o proceso, habilidad o capacidad, o estado mediante el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso o modificación no autorizados, o explotación.[4]

Denegación de servicio distribuida (DDoS, por sus siglas en inglés): tipo de ataque cibernético en la que el atacante hace que la máquina, el sitio web o la red objetivo no estén disponibles para sus usuarios al inundar el objetivo con solicitudes en un intento de sobrecargar el sistema.

Cifrado: El proceso de transformar texto sin formato en texto cifrado.[5]

Firewall: Capacidad que limita el tráfico de red entre redes y/o sistemas de información.[6]

Firmware: Programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante la ejecución.[7]

HTTPS: una combinación del Protocolo de Transferencia de Hipertexto (HTTP, por sus siglas en inglés) con el protocolo de Capa de Puertos Seguros (SSL, por sus siglas en inglés) /Seguridad de la Capa de Transporte (TLS, por sus siglas en inglés). TLS es un protocolo de autenticación y seguridad ampliamente implementado en navegadores y servidores web.[8]

Malware: software que compromete el funcionamiento de un sistema al realizar una función o proceso no autorizado.[9]

Módem: dispositivo que convierte datos digitales para transmitirlos en una red; por ejemplo, un dispositivo que permite que una red doméstica o comercial se conecte con un proveedor de servicios de Internet (ISP, por sus siglas en inglés).

Autenticación multifactor: Autenticación que utiliza dos o más factores diferentes para lograr la autenticación. Los factores incluyen: algo que sabe (por ejemplo, contraseña o PIN); algo que tiene (p. ej., dispositivo de identificación criptográfica o token); o algo que eres (por ejemplo, biometría).[10]

Enrutador: en una red, un dispositivo que determina la mejor ruta para reenviar un paquete de datos hacia su destino;[11] — por ejemplo, un dispositivo que emite una señal Wi-Fi.

Capa de Puertos Seguros (SSL, por sus siglas en inglés: proporciona privacidad e integridad de datos entre dos aplicaciones que se comunican entre sí. Está diseñado para encapsular otros protocolos, como HTTP.[12]

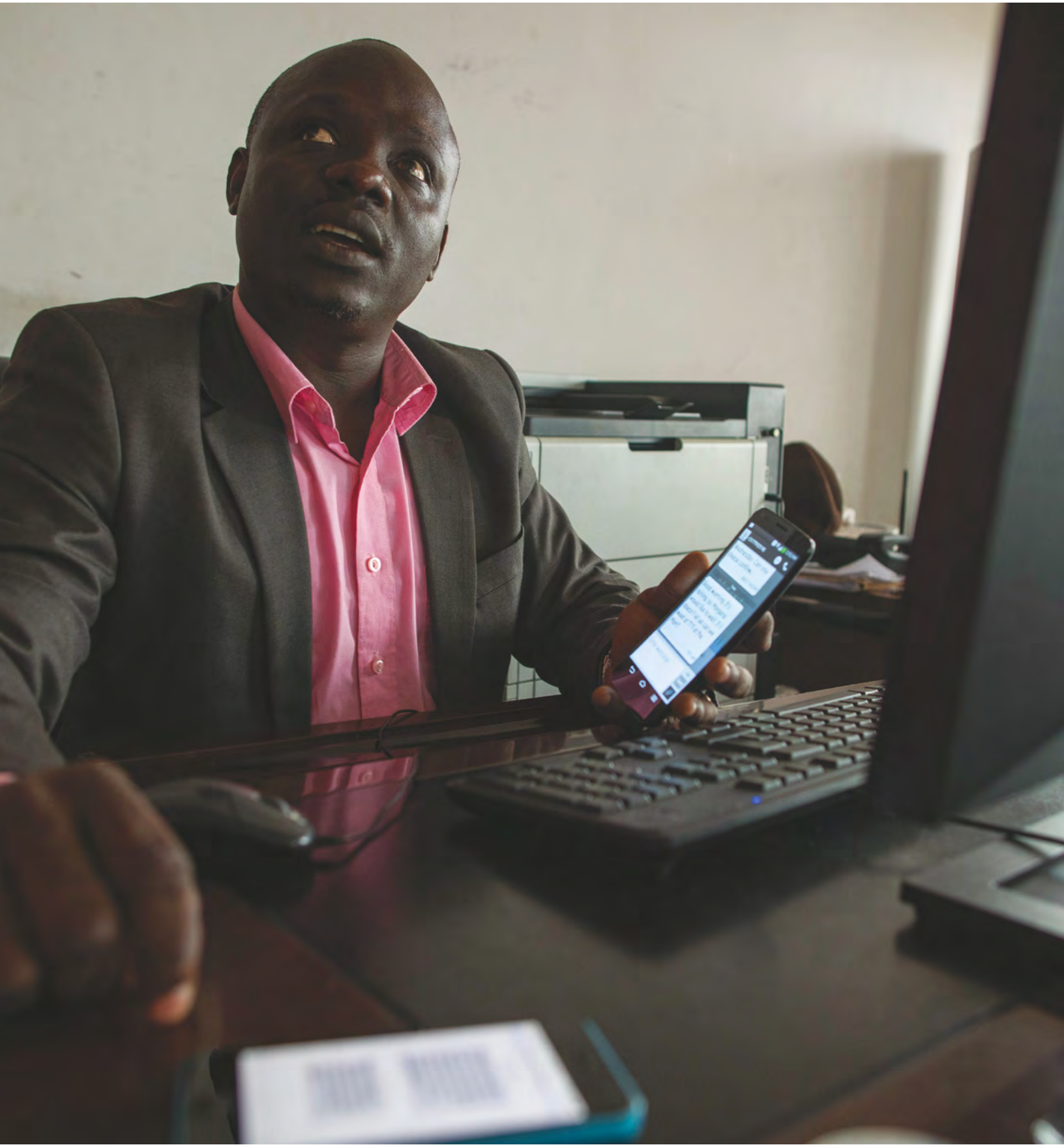
Identificador de conjunto de servicios (SSID, por sus siglas en inglés): el nombre de una red Wi-Fi.

Acceso Wi-Fi Protegido 2 (WPA2): Protocolo de seguridad que utiliza contraseñas para proteger redes Wi-Fi.

LISTA DE ACRÓNIMOS

DDoS	Denegación de Servicio Distribuida
IoT	Internet de las Cosas
IP	Protocolo de Internet
ISP	Proveedor de Servicios de Internet
IT	Tecnología de Información
NIST CSF	Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología
PCI	Industria de Tarjetas de Pago
SSID	Identificador de Conjunto de Servicios
SSL	Capa de Puertos Seguros
WPA	Acceso Wi-Fi Protegido
WPS	Configuración de Wi-Fi Protegido

1 https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
2 https://www.oed.com/
3 https://csrc.nist.gov/glossary
4 https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
5 https://csrc.nist.gov/glossary
6 https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
7 https://csrc.nist.gov/glossary
8 https://www.healthit.gov/faq/what-does-https-web-address-mean
9 https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
10 https://csrc.nist.gov/glossary
11 https://csrc.nist.gov/glossary
12 https://www.oed.com/



INTRODUCCIÓN

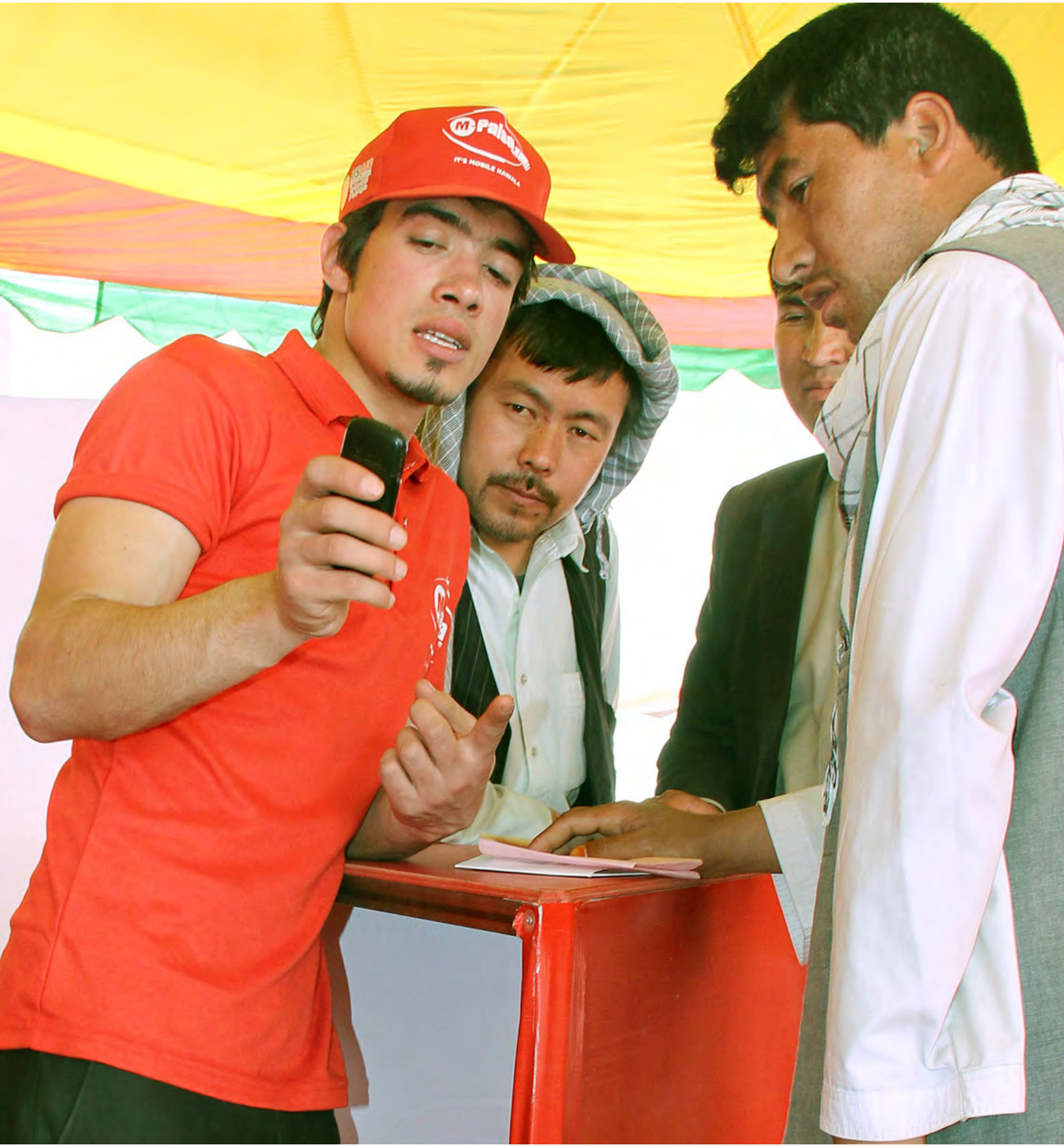
Esta segunda sección de la *Guía de Ciberseguridad para Pequeñas y Medianas Empresas* presenta un rango de estrategias prácticas que los propietarios de pequeñas empresas pueden implementar para proteger a sus organizaciones de amenazas de ciberseguridad. Este punto de partida puede ayudar a los propietarios a sentirse más cómodos con las ideas y estrategias que explora esta guía. Para mayor profundidad, los propietarios de pequeñas empresas deben consultar recursos más avanzados en Internet o buscar el consejo de un profesional de TI.

Desde el punto de vista de una empresa, puede parecer lógico abordar la ciberseguridad únicamente desde una perspectiva de cumplimiento legal. Si bien este puede ser un primer paso en la dirección correcta, las empresas deben asumir que la innovación y las nuevas tecnologías superan rápidamente las regulaciones. Hay acciones relativamente simples que las empresas pueden tomar para reducir en gran medida la probabilidad y el impacto de los ataques cibernéticos. Al mismo tiempo, a pesar de las mejores prácticas preventivas, es probable que al menos un ataque tenga éxito, por lo que es necesario crear resiliencia dentro de la empresa y establecer la capacidad de recuperarse después de una infracción.

La Importancia de un Buen Líder

Las organizaciones de todos los tamaños se cuestionan quién debe liderar la ciberseguridad. El artículo de Harvard Business Review sobre cómo reformular el liderazgo en ciberseguridad argumenta que la persona que lidera y es responsable de la ciberseguridad en la organización debe ser "una voz influyente en la estrategia empresarial, las decisiones tecnológicas y la gestión de riesgos empresariales", en lugar de alguien que solo tiene el dominio técnico.[13] Las empresas deben incorporar la concienciación sobre ciberseguridad y las buenas prácticas en toda la organización, cubriendo todos los elementos: técnica, estrategia de planificación empresarial y personas, incluyendo clientes, proveedores y empleados.

13 https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is



© FAIDA

DÓNDE EMPEZAR

Es probable que muchas empresas ya estén implementando algunos pasos de ciberseguridad como parte de una postura de seguridad de TI que, si se complementa, puede reducir en gran medida el riesgo. Estas acciones, conocidas como higiene cibernética", son relativamente simples, se realizan de forma rutinaria y pueden tener un impacto positivo en la seguridad digital de las empresas. Las mejores prácticas de ciberhigiene incluyen:

1. Capacitar a empleados para que confíen, pero verifiquen;
2. Instalar un software antivirus y antimalware confiable y mantenerlo actualizado;
3. Usar cortafuegos de red y revisarlos periódicamente;
4. Elegir contraseñas seguras y cambiarlas con frecuencia;
5. Utilizar la autenticación multifactor;
6. Actualizar el software de manera regular;
7. Cifrar todos los datos confidenciales;
8. Asegurar las conexiones Wi-Fi;
9. Supervisar los sistemas de pago;
10. Mantener seguro el sitio web de la empresa;
11. Evitar que los teléfonos móviles sean objetivo de ataque;
12. Mantener copias de seguridad de toda la información;
13. Recordar que seguridad física es parte de ciberseguridad;
14. Explorar la posibilidad de un seguro cibernético; y
15. Considerar contratar a un profesional de TI.

CAPACITACIÓN DE EMPLEADOS

La capacitación de los empleados es indispensable para el éxito de la empresa y debe incluir la concienciación sobre ciberseguridad. La capacitación de nuevos empleados debe presentarles las habilidades y los sistemas necesarios para sus funciones laborales, incluyendo seguridad cibernética básica. La capacitación continua y las certificaciones o actualizaciones anuales preparan a los empleados para el entorno empresarial cambiante, y deben cubrir las actualizaciones de las políticas, estrategias y tácticas de seguridad cibernética para mitigar las nuevas amenazas.

1. Capacitar a los empleados a confiar, pero verificar

Como regla general, los empleados solo deben tener acceso a los recursos y la información necesarios para realizar sus funciones laborales. Para determinar esto, una empresa necesita saber cómo se utilizan los datos, sistemas, dispositivos, etc. y con qué propósito. Siempre que sea posible, las empresas deben crear perfiles de usuario, es decir, cuentas que limiten el acceso a recursos específicos dentro de la empresa. Cuando esto no es posible, la siguiente mejor opción es establecer restricciones y proteger con contraseña el acceso a carpetas o archivos como parte de la funcionalidad de los sistemas operativos.

La clave para limitar el acceso también es cancelar el acceso una vez que un empleado deja la empresa. Esto mitigará el riesgo de amenazas internas. Si una empresa quiere controles robustos, existen muchas soluciones de TI que pueden facilitar la creación y gestión de perfiles de usuario. Los administradores pueden hablar con un profesional de TI y deberían considerar ponerse en contacto con el servicio de asistencia de su sistema operativo para saber qué métodos de control de acceso a archivos son adecuados.

MITIGANDO RIESGOS: CUENTAS DE USUARIOS

Después de comprender cuál es la información de la empresa y cómo puede poner en riesgo a la organización, las empresas deben identificar quién tiene acceso a qué datos. Deberían:

- **Reunir una lista completa de cuentas de usuario** utilizadas para acceder a todos los servicios, dispositivos, aplicaciones, direcciones de correo electrónico, servicios en la nube, bases de datos, teléfonos, tabletas, dispositivos de Internet de las cosas (IoT, por sus siglas en inglés), sistemas empresariales, etc. Necesitan saber y registrar quién los usa, incluidos los proveedores externos que tienen acceso.
- **Identificar a cada usuario y los flujos de datos a los que tiene acceso, y exija el uso de contraseñas diferentes para cada función o sistema**, especialmente para aquellos que contengan información restringida.
- **Indicar a los usuarios que no compartan cuentas y que protejan con contraseña los datos críticos.**

SUSCRIPCIONES GRATUITAS VS PAGADAS

Muchas empresas de seguridad de renombre ofrecen versiones gratuitas de programas antivirus y cortafuegos. Teniendo en cuenta el nivel de riesgo empresarial, estas versiones pueden ser una defensa suficiente para empresas con menor riesgo. Para aquellas con mayor riesgo, las suscripciones pagadas pueden ser necesarias para otorgar funcionalidad o soporte adicional.

CONFIGURACIÓN DE CORTAFUEGOS

Pruebe el contrafuegos al configurar el plan de ciberseguridad empresarial. Esto ayudará a garantizar que esté correctamente configurado y funcionando. Aunque hay varias herramientas gratuitas en línea que pueden ayudar a realizar pruebas, puede ser prudente trabajar con un profesional de TI que pueda interpretar los resultados técnicos y solucionar los problemas identificados.

2. Instalar un software antivirus y antimalware confiable

La solución más común para protegerse contra el malware es un software antivirus. Los sistemas operativos Microsoft Windows, Google Chrome y Mac ya tienen un software antivirus integrado que funciona bien contra la mayoría de las amenazas[14] y que tiene la funcionalidad básica para detectar y eliminar malware, cuando están actualizados. A pesar de las ventajas de estos programas integrados, los atacantes tienen amplias oportunidades para diseñar programas de malware para eludir estas defensas. Es una buena práctica incluir protección antivirus adicional en los dispositivos de TI de la empresa y asegurarse de que se actualice de manera regular.[15]

3. Usar cortafuegos de red

Los cortafuegos o "firewalls" son dispositivos o programas que controlan el flujo de información o tráfico entre redes (tráfico de red) desde una red externa a la empresa, dentro de la red interna de la empresa, o entre dispositivos con diferentes configuraciones

de seguridad.[16] Los cortafuegos se pueden integrar en el enrutador proporcionado por el proveedor de servicios de Internet (ISP, por sus siglas en inglés) o en programas antivirus específicos. Un cortafuegos es una defensa esencial para una empresa. Según el nivel de riesgo empresarial, las empresas deben considerar si actualizar los cortafuegos y complementarlos con otras soluciones, como aquellas que cifran el tráfico o monitorean de cerca la información intercambiada con y dentro de la red empresarial.

4. Elegir contraseñas seguras

Las contraseñas simples de una sola palabra que se usaban en el pasado ya no son un medio efectivo para proteger una cuenta. Los atacantes ahora tienen herramientas capaces de descifrar contraseñas en una hora o menos. Una práctica más segura es desarrollar contraseñas con frases cortas que contengan números y caracteres especiales mixtos para que las contraseñas sean más complejas, largas y difíciles de adivinar. Ejemplos de ese tipo de contraseñas son **#SI33pWe11**, **Sc0r3G0a1!**, y **K0mbuchaP0w3r***.

MITIGANDO RIESGOS: PROTECCIÓN DE CONTRASEÑAS

Las contraseñas siempre deben ser complejas, guardarse en un lugar seguro, mantenerse confidenciales y cambiarse regularmente. Una de las vulnerabilidades más comunes para las empresas es que los empleados escriban su contraseña en una nota adjunta a su computadora o en algún otro lugar cerca de su área de trabajo, lo que amenaza la seguridad de los datos. Las "carteras" digitales cifran de forma segura las contraseñas guardadas.

Las empresas deben tener una contraseña para cada sistema o sitio web y deben asegurarse de que se cambien con regularidad o al menos una vez al año. Si un sitio permite contraseñas más largas (20 o más caracteres), los usuarios pueden crear oraciones de contraseña completas, como "¡Me gustarían unas largas vacaciones!".

Las interfaces administrativas de los sistemas por lo general permiten la personalización de los requisitos de contraseña, incluyendo la frecuencia para cambiarlos. Las empresas deben usar esas funcionalidades para crear especificaciones de contraseña que funcionen para la seguridad deseada de la organización.

14 https://www.av-test.org/en/antivirus/home-windows/

15 Publicaciones conocidas, como *PC Magazine*, realizan con frecuencia pruebas en software antivirus y cortafuegos gratuitos e informan de sus hallazgos al público. Pueden encontrar ejemplos de las revisiones aquí: https://www.pcmag.com/picks/the-best-free-antivirus-protection

16 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

5. Utilizar la autenticación multifactor

El uso de la autenticación multifactor se ha vuelto popular en los últimos años. La "autenticación multifactor" requiere que los usuarios proporcionen dos o más medios de verificación para obtener acceso a una cuenta, aplicación o sistema. Puede ser una combinación de una contraseña u otra información específica del usuario legítimo y un código generado y enviado por el sistema (por correo electrónico, mensaje de texto o llamada telefónica) al usuario. Muchas plataformas de tecnología, incluyendo los proveedores de inicio de sesión único, los sistemas de pago y varias cuentas de usuario, ahora utilizan la autenticación multifactor. Si está disponible, las empresas deben asegurarse de que esté habilitado para cuentas internas (empleados) y externas (clientes), según corresponda.

6. Actualizar el software de manera regular

Con las actualizaciones, los desarrolladores solucionan o "parchan" problemas, como vulnerabilidades de seguridad conocidas de aplicaciones, programas o sistemas operativos. Estas actualizaciones deben instalarse lo antes posible. Las empresas deben tener en cuenta que los desarrolladores solo pueden corregir las vulnerabilidades conocidas. Si un problema no se detecta, una empresa será vulnerable, incluso si todos sus sistemas de TI se actualizan de manera constante. Este es un riesgo para el que hay que estar preparado, pero la actualización periódica del software empresarial mitigará gran parte de ese riesgo.

7. Cifrar todos los datos confidenciales

El cifrado de datos hace que el contenido sea legible solo para aquellos que tienen las claves o contraseñas para abrir o descifrar los datos. Se pueden cifrar archivos individuales o dispositivos completos, incluyendo las unidades en la nube. Hay muchas soluciones de cifrado disponibles, y tanto Microsoft como Apple ofrecen herramientas de cifrado integradas, como BitLocker[17] y FileVault[18], respectivamente. La desventaja de estas herramientas es que, si se pierde la clave o contraseña, los datos no se pueden recuperar. Asegúrese de hacer una copia de la clave en un lugar seguro o tenga una forma segura de recordar la contraseña asociada.

8. Asegurar las conexiones Wi-Fi

Los ISP generalmente proporcionan dispositivos Wi-Fi como cajas que tienen un "módem" (el equipo que conecta la empresa a la red del proveedor) y un "enrutador" (el equipo que transmite la señal de Wi-Fi dentro de la empresa) combinado en uno. Por lo general, un técnico instala esta caja en la instalación inicial de Internet y la caja permanece intacta hasta que el ISP la cambia o el equipo falla y necesita ser reemplazado. Los ISP compran grandes cantidades de estos dispositivos, y sus consideraciones de seguridad para los consumidores no necesariamente se alinean con los requisitos de seguridad de una empresa en particular. Es probable que los dispositivos deban adaptarse para satisfacer

las demandas de ciberseguridad de una empresa. Para aumentar la protección que puede brindar un enrutador, existen algunas acciones que se pueden realizar con poco o ningún costo:

a. **Cambie la contraseña para acceder a la configuración del enrutador ISP.** El enrutador tiene una interfaz que permite a los administradores realizar cambios en la configuración del dispositivo. Los enrutadores vienen con una contraseña genérica asignada por un ISP para acceder a su configuración. Siguiendo las instrucciones del manual del dispositivo, los administradores pueden cambiar la contraseña genérica por una contraseña nueva y segura. Se debe guardar esa nueva contraseña en un lugar seguro y solo compartirla con las personas adecuadas.

b. **2. Actualice el firmware del enrutador ISP de la empresa con regularidad.** "Firmware" es el sistema operativo del enrutador. Con el conocimiento para acceder a la configuración del enrutador, los administradores siguen las instrucciones del fabricante para buscar e instalar actualizaciones. De acuerdo con el plan de ciberseguridad empresarial, verifican de manera periódica si hay nuevas actualizaciones y las instalan según sea necesario. Necesitan ubicar la fecha de término del soporte del dispositivo y planificar con anticipación para reemplazarlo en ese momento.

c. **Habilite siempre la seguridad, es decir, el protocolo de encriptación**, para conectarse a Wi-Fi y cambie con frecuencia la contraseña para acceder a él. Si el enrutador admite una red de invitados, los administradores deben habilitarlo y usarlo para cualquier persona o cosa que no necesite acceso a los sistemas de TI de la empresa, incluyendo invitados, proveedores externos y dispositivos IoT privados. Los protocolos de encriptación Wi-Fi aseguran la conexión entre el enrutador y el dispositivo que se conecta a él, como una computadora portátil, pero no las comunicaciones a través de Internet. Esto hace que también sea necesario cambiar con frecuencia la contraseña de la red de invitados. El cifrado Wi-Fi está en constante evolución con Acceso Wi-Fi Protegido (WPA, por sus siglas en inglés) y su reemplazo más seguro, WPA2, ahora comúnmente admitido por dispositivos. Las empresas deben habilitar el protocolo más avanzado posible y reemplazar la contraseña Wi-Fi predeterminada por una contraseña segura y única, incluso si la predeterminada parece difícil de descifrar. WPA2 acepta un rango de 8 a 63 caracteres, que debería ser suficiente para admitir contraseñas de red, como **MaryHadaLittleLamb,LittleLamb,LittleLamb,MaryHadaLittleLamb**. La realidad es que las contraseñas Wi-Fi empresariales a menudo se comparten con personas externas, por lo que es una buena práctica cambiarlas con regularidad como parte del plan de ciberseguridad empresarial y garantizar que la contraseña interna, que no es de invitado, sea segura y no se publique.

d. **Deshabilite la conexión Wi-Fi fácil.** Un ejemplo es la tecnología Configuración de Wi-Fi Segura (WPS, por sus siglas en inglés) de un solo botón. Si el enrutador no está protegido físicamente, cualquier persona que tenga acceso físico al enrutador puede usar esta función para penetrar en su red.

17 https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838

18 https://support.apple.com/en-us/HT204837

e. **Cambie el nombre del Wi-Fi.** El Identificador de conjunto de servicios (SSID) es el nombre del Wi-Fi. Cambia el SSID por defecto por uno que no revele información personal y que no proporcione información sobre el dispositivo que se utiliza, como la marca y el modelo del enrutador o el ISP, para no facilitar un ataque.

f. **Investigue las implicaciones antes de realizar otros cambios en el enrutador.** Habilitar o deshabilitar una funcionalidad puede abrir o cerrar puertas a ataques o limitar la funcionalidad del dispositivo.

g. **Pruebe.** Después de implementar los cambios, ejecute pruebas para ver si funcionan según lo previsto.

h. **Agregue su propio enrutador.** No es inusual que los entornos de pequeñas empresas reciban enrutadores de nivel de consumidor, y los ISP reservan equipos más sofisticados para clientes más grandes. Una pequeña empresa puede mejorar su seguridad Wi-Fi y su control sobre la funcionalidad del enrutador agregando su propio enrutador conectado al enrutador/módem proporcionado por el ISP. Los administradores pueden ponerse en contacto con el ISP para analizar cómo implementar esta configuración o buscar opciones en los fabricantes.

9. Supervisar los sistemas de pago

Según el modelo de la pequeña empresa, los pagos se recibirán de diferentes maneras, por ejemplo, a través del punto de venta, el sitio web de la empresa, una aplicación o el sitio de una empresa externa, y cada uno presenta desafíos específicos para la seguridad cibernética. El Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés), una organización que desarrolla estándares de seguridad relacionados con los métodos de pago, ha creado guías completas[19] sobre los riesgos potenciales de estos diferentes sistemas, incluyendo los terminales de pago conectados a Internet o las aplicaciones de pago. Las guías también aconsejan sobre las acciones que se pueden tomar para mitigar el riesgo. Muchas de las acciones de mitigación se relacionan con prácticas de higiene cibernética (por ejemplo, actualización de software y uso de contraseñas seguras) porque los sistemas de pago también son dispositivos conectados. El cifrado de los datos de la tarjeta de pago del consumidor durante el tránsito al procesador de pagos y dentro de los sistemas empresariales es de especial importancia.

SEGURIDAD FÍSICA

La ciberseguridad tiene como objetivo brindar protección en el mundo digital, pero la ciberseguridad y la seguridad física se superponen. Cualquiera que tenga acceso a un terminal de pago puede manipularlo. Si un hacker tiene acceso físico a un enrutador, puede robar las credenciales de inicio de sesión en la red de la empresa. Esta guía no analiza los procedimientos de la seguridad física, pero las empresas deben tener en cuenta que una estrategia de ciberseguridad integral y exitosa debe incluir la seguridad física de las instalaciones, las redes y los dispositivos.

10. Mantener el sitio web de la empresa seguro

Un sitio web es una herramienta para interactuar con los consumidores, brindar servicios o vender productos, y establece en gran medida la identidad digital de una empresa. La mejor manera de proteger este activo crítico depende de las propiedades técnicas del sitio, el ecosistema de TI en el que se administra y dónde se guarda o aloja el sitio. Muchas empresas utilizan servicios en la nube que ofrecen herramientas de creación de sitios web fáciles de usar. Estas soluciones alivian la carga de crear y administrar el sitio y transfieren parte de la responsabilidad de proteger y monitorear la infraestructura de TI al proveedor del servidor. Sin embargo, los sitios web aún pueden estar en riesgo si están codificados de manera incorrecta por la herramienta de creación, los complementos,

las extensiones o los servicios de terceros que están configurados incorrectamente o tienen vulnerabilidades.

MITIGANDO RIESGOS: SEGURIDAD DEL SITIO WEB

Haga coincidir el nivel de asignación de recursos necesarios para proteger el sitio web empresarial con el nivel de importancia del sitio web para la empresa y los riesgos inherentes. Es una buena práctica:

1. **Tenga requisitos sólidos para las credenciales de inicio de sesión del administrador.** Limite el número de personas que tienen privilegios de administrador.
2. **Utilice un software de creación y alojamiento de sitios web de buena reputación para desarrollar y mantener el sitio.**[20] Es probable que las empresas de renombre tengan buenas suites de seguridad, como contrafuegos, antimalware, monitoreo y opciones de prevención de denegación de servicio distribuida (DDoS)[21] para proteger los sitios alojados y las características escalables.
3. **Actualice con regularidad el software del sitio.** Esto incluye la plataforma, el software del sitio web y cualquier programa adicional codificado en el sitio, por ejemplo, complementos, extensiones e integraciones de terceros.
4. **Utilice protocolos HTTPS.** Esto requiere la instalación de certificados de capa de puertos seguros (SSL) que cifran la información entre el sitio web y el usuario.
5. **Solicite contraseñas seguras si el sitio web permite a los usuarios crear cuentas** y habilite funcionalidades para bloquear cuentas después de varios intentos fallidos de inicio de sesión.
6. **Cree un "cyber pen" alrededor de los archivos que cargan los usuarios.** Esto requiere contar con medidas para garantizar que los archivos estén seguros, incluyendo escáneres antivirus y antimalware de un tipo permitido. Es recomendable limitar el tipo y el tamaño de los archivos que se aceptan para cargar y tener un programa que verifique el tipo de archivo y garantice que el archivo se cargue en una ubicación segura fuera de la carpeta donde se almacena información confidencial o donde hay acceso a todos los archivos del sitio web.
7. **Realice una copia de seguridad periódica del sitio, que incluya todos sus datos.** La frecuencia de las copias de seguridad depende de la importancia de los datos, pero lo ideal es que las copias de seguridad se realicen a diario. Si es posible,

19 https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf

20 Empresas como Wix, Squarespace o Weebly han sido reconocidas a nivel mundial por sus productos y servicios. Puede haber otras empresas nacionales o regionales que puedan ofrecer productos comparables.

21 La denegación de servicio distribuida (DDoS) es una forma de ataque cibernético que abruma a un servidor objetivo con solicitudes que eventualmente resultan en que ese objetivo rechace las solicitudes de servicio legítimas. Esto termina deshabilitando el sitio web.

22 https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

23 https://support.apple.com/guide/icloud/erase-a-device-mmfc0ef36f/icloud

24 https://support.google.com/accounts/answer/6160491?hl=en

la empresa debe tener un servicio automático de copias de seguridad. En los casos en que el sitio web y sus datos sean críticos para la empresa, las organizaciones deben considerar realizar copias de seguridad redundantes y mantener los datos de copia de seguridad en diferentes ubicaciones para tener acceso a los datos en caso de un desastre natural o político o un ataque cibernético.

11. Evitar que los teléfonos móviles sean objetivos de ataque

El número de usuarios de teléfonos inteligentes aumenta constantemente, con más de 3.400 millones estimados actualmente en todo el mundo.[22] Muchos usuarios de teléfonos inteligentes llevan dispositivos al lugar de trabajo o utilizan los proporcionados por los empleadores. Lo que diferencia a los dispositivos móviles de las computadoras del trabajo es la cantidad de datos personales y de trabajo que los dispositivos pueden guardar y que siempre están en línea. Además, su portabilidad los pone en mayor riesgo de pérdida o robo. Un hacker que puede acceder a un teléfono, ya sea físicamente o infectándolo con malware, puede penetrar en la red de una empresa. Tenga en cuenta que una empresa tiene más control sobre los dispositivos móviles que proporciona a sus empleados que sobre los dispositivos personales que esos empleados traen al entorno empresarial.

MITIGANDO RIESGOS
ASEGURANDO LOS DISPOSITIVOS MÓVILES

Las empresas pueden mejorar la seguridad de los dispositivos móviles siguiendo prácticas generales de higiene cibernética (por ejemplo, actualizar aplicaciones y sistemas operativos, instalar programas de buena reputación, configurar para usar conexiones seguras, usar redes Wi-Fi confiables, etc.). Además, hay algunas precauciones que se aplican solo a los teléfonos inteligentes. Las empresas deben:

1. **Usar y actualizar el sistema operativo del fabricante.** Un método común para limpiar un teléfono es usar una interfaz basada en web administrada por el fabricante del dispositivo o el desarrollador del sistema operativo. Tanto Apple[23] como Android tienen esta funcionalidad.[24] La seguridad sólida permite que un usuario cifre toda la información almacenada en el teléfono con una copia de seguridad en la nube o en una computadora personal, y se requiere una contraseña segura o información biométrica para desbloquear el teléfono. Las empresas deben utilizar todos estos métodos.
2. **Use and update the manufacturer's operating system.** A menudo, los usuarios reemplazan el sistema operativo original con uno creado por una comunidad de desarrolladores. Este proceso se llama "rooting" o "jailbreaking". Dado que la seguridad de un sistema operativo rooteado y con jailbreak es difícil de garantizar, esos dispositivos no deben tener acceso a la red de la empresa ni a datos confidenciales.

3. **Evite hacer clic en enlaces sospechosos, especialmente en aplicaciones de mensajería o de texto.** Como se explicó en la sección anterior, los enlaces en los mensajes pueden contener malware y lanzar un ataque.
4. **Esté atento a las aplicaciones y restrinja los datos a los que pueden acceder las aplicaciones.** Los investigadores analizan de forma rutinaria las aplicaciones en busca de problemas de seguridad, como en el conocido debate reciente que involucra a TikTok y WeChat.[25] Evitar aplicaciones fuera de las tiendas oficiales del sistema operativo (por ejemplo, Google Play y Apple App Store) y restringir los datos a los que pueden acceder las aplicaciones después de la instalación son buenas prácticas de ciberseguridad. Las empresas deben tratar de limitar el acceso de las aplicaciones a otros recursos, como la ubicación, los contactos, las carpetas de archivos, la información de otras aplicaciones y la cámara.
5. **Desactive las funciones cuando no las utilice.** Los teléfonos inteligentes tienen muchas formas de conectarse, además de las redes celulares, incluyendo Bluetooth, Wi-Fi y AirDrop. Cada uno de estos son caminos potenciales para un ataque. Los administradores solo deben activar las funcionalidades necesarias cuando sea necesario.
6. **Eliminar.** Después de desconectar un teléfono celular de la red de una empresa, se deben eliminar todos los datos relacionados con la empresa. Si es posible, el teléfono celular debe limpiarse por completo de todos los datos.

12. Mantener copias de seguridad de toda la información

Actualmente, la mayoría de las empresas dependen en gran medida de los datos y los sistemas de tecnología de la información (TI). Al planificar la seguridad cibernética y crear copias de seguridad, las organizaciones deben comprender cómo funcionan los sistemas y deben priorizar las copias de seguridad para la información más confidencial y los sistemas críticos. A medida que la empresa madura, los administradores deben comenzar a pensar en obtener sistemas más sofisticados que ayuden a recuperar las operaciones más rápidamente después de un incidente.

Con la llegada del almacenamiento en la nube gratuito y asequible, algunas empresas creen que estos sistemas brindan una copia de seguridad adecuada. Si bien la mayoría brinda respaldo, si el almacenamiento en la nube se sincroniza con una computadora, un ataque al sistema, archivo o servicio en la nube original puede extenderse a los datos almacenados adicionales, por lo que ese tipo de protección por sí solo podría no ser suficiente. Las empresas deben aprovechar al máximo las soluciones en la nube gratuitas de buena reputación como un paso inicial para proteger los datos. También deben tomar en cuenta las limitaciones, que incluyen su inadecuación para realizar copias de seguridad de ciertos tipos y tamaños de archivos, la incompatibilidad con los nombres de los archivos y la posibilidad de perder datos desde el momento en que se guardaron por

COSTOS DE UNA INACTIVIDAD

En 2014, la compañía de investigación global Gartner descubrió que el costo promedio del tiempo de inactividad comercial era de $5.600 por minuto. Para una empresa, este costo puede ser menor, dependiendo de las características de la organización, el país y el sector, pero es razonable estimar que sin un plan de ciberseguridad, los costos de volver a poner la empresa en línea ascenderán a varios días de costos operativos, incluso en el mejor de los casos.

25 https://www.vox.com/recode/2020/8/11/21363092/why-is-tiktok-national-security-threat-wechat-trump-ban

última vez hasta el momento de la próxima copia de seguridad.[26] Un buen ejemplo es una pequeña empresa que produce videos. Esos archivos son muy grandes, difíciles y lentos para realizar copias de seguridad en los servicios en la nube. Perder días o semanas de datos no guardados puede resultar muy costoso. En algunos países, las soluciones gratuitas pueden no ser adecuadas para cumplir con las regulaciones.[27]

Una buena estrategia de respaldo debe guardar programas y sistemas operativos, no solo datos. En otras palabras, debe tener como objetivo crear una copia o imagen completa de toda la información en los discos duros utilizados por las computadoras de la empresa. En caso de incidente, esa imagen se puede volver a cargar en una computadora limpia o nueva, lo que reduce el tiempo de recuperación.[28] Mediante el uso de software especializado, las copias de seguridad se pueden guardar de manera local (en el almacenamiento propio de la computadora), en unidades o medios externos, en un servicio en la nube o en un escenario híbrido usando almacenamiento local y en la nube.

MITIGANDO RIESGOS: RESPALDOS DE DATOS

Las empresas deben realizar copias de seguridad de sus datos con frecuencia y, si es posible, de forma automática. Si la organización no tiene una solución automática, necesita presupuestar el tiempo para crear de forma manual copias de seguridad completas. Ese es un factor cuando se considera el nivel de tolerancia a la pérdida de datos aplicable a una empresa. Los sistemas operativos de Microsoft y Apple, así como muchos sistemas operativos móviles, ofrecen funciones de copia de seguridad que pueden utilizarse como punto de partida.

Las copias de seguridad pueden corromperse o perderse, o los medios utilizados para guardarlas pueden quedar obsoletos, por lo que es aconsejable hacer varias copias utilizando diferentes medios. Una copia debe mantenerse fuera del sitio para protegerla de un incidente catastrófico, como un incendio o el derrumbe de un edificio, y todas las copias deben estar cifradas.

Algunas empresas pueden tener el desafío adicional de la falta de interconexión o estandarización de sus sistemas. Es posible que no todos los empleados tengan la misma computadora o sistema operativo, y la información empresarial podría distribuirse entre computadoras y dispositivos adaptados a las funciones individuales de los empleados. Por ejemplo, el contador tiene toda la información contable, la persona de mercadotecnia tiene toda la información de mercadotecnia, etc. En esos casos, la creación de copias de seguridad manuales puede ser la única opción factible, a menos que la empresa esté preparada para invertir en una infraestructura de TI que pueda admitir todos los dispositivos.

13. Recordar que la seguridad física es parte de la ciberseguridad

Los activos físicos de TI representan una cantidad significativa de riesgo. Conectar, desconectar, reiniciar y cargar son algunas de las muchas acciones que un atacante puede realizar para facilitar o lanzar un ataque cibernético cuando tiene acceso físico a los dispositivos empresariales. Las computadoras con la información empresarial más confidencial deben guardarse en un lugar seguro, como un gabinete u oficina cerrados. Un enrutador no debe dejarse sin seguridad en un área de acceso abierto. Las empresas deben asegurarse de que los dispositivos industriales conectados requieran llaves para funcionar. Para determinar qué dispositivos son críticos, como mínimo, una empresa debe saber qué dispositivos tiene, para qué se utilizan y el tipo de información que se almacena en ellos.

Es probable que la mayoría de las empresas ya cuenten con protocolos de seguridad física sólidos, y las medidas requeridas dependen del tipo de empresa y su ubicación. Lo importante es incluir los ciberactivos en la seguridad física del negocio.

14. Explorar la posibilidad de un seguro cibernético

En algunos mercados, las compañías de seguros ofrecen pólizas que cubren las pérdidas resultantes de un ataque cibernético, como una interrupción de la red o una filtración de datos. El seguro cibernético no debe verse como un reemplazo de una seguridad cibernética adecuada. Cuando esté disponible, este seguro puede ser una herramienta valiosa para mitigar daños y fortalecer las defensas cibernéticas, pero no elimina el riesgo ni cubre todas las consecuencias y costos de los riesgos o incidentes cibernéticos.

Al tomar la decisión de comprar un seguro y de qué tipo, las empresas deben considerar su perfil de riesgo específico y no lo que tienen otras empresas, incluso si son similares. Tomemos el ejemplo de una empresa que ofrece una entrega garantizada de productos a tiempo. Si un ataque cibernético a esa empresa le impide entregar el producto a tiempo, la empresa tendrá una mayor exposición a la responsabilidad que sus competidores.

REVISAR LA HIGIENE CIBERNÉTICA

Las organizaciones necesitan identificar prácticas y políticas de higiene cibernética adecuadas. Los administradores pueden considerar los puntos 1 a 13 en esta sección de la guía y determinar la guía más relevante para los tipos de información y sistemas del negocio. Además, deben considerar si la empresa está utilizando la mayor cantidad posible de esta guía y luego identificar las áreas de mejora y cómo implementar estas actualizaciones.

26 Cuando hay un incidente, incluso si una empresa realiza copias de seguridad periódicas, siempre pierde algunos de sus datos. Si se realiza una copia de seguridad diariamente al cierre de operaciones del viernes y se produce un ataque al final del lunes, la pérdida sería de 72 horas.

27 https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

28 *PC Magazine* revisa regularmente los servicios de respaldo y los califica de acuerdo con diferentes puntos de referencia https://www.pcmag.com/picks/the-best-online-backup-services

MITIGANDO LOS RIESGOS:
COBERTURA DE SEGURO PARA LA EMPRESA

Las empresas con pólizas de seguros comerciales deben comunicarse con su aseguradora para determinar si se cubren los ataques cibernéticos o las pérdidas provocadas por un incidente cibernético, como la pérdida de datos debido al robo por parte de un empleado. Las organizaciones también pueden consultar sobre cobertura cibernética adicional y si, como parte de la póliza de seguro, la aseguradora ofrece apoyo para mejorar las prácticas de ciberseguridad del titular de la póliza. Estos servicios a veces se ofrecen para reducir los riesgos de una aseguradora. Las empresas deben tener en cuenta los siguientes puntos al analizar la cobertura con una aseguradora y al considerar la compra de una póliza

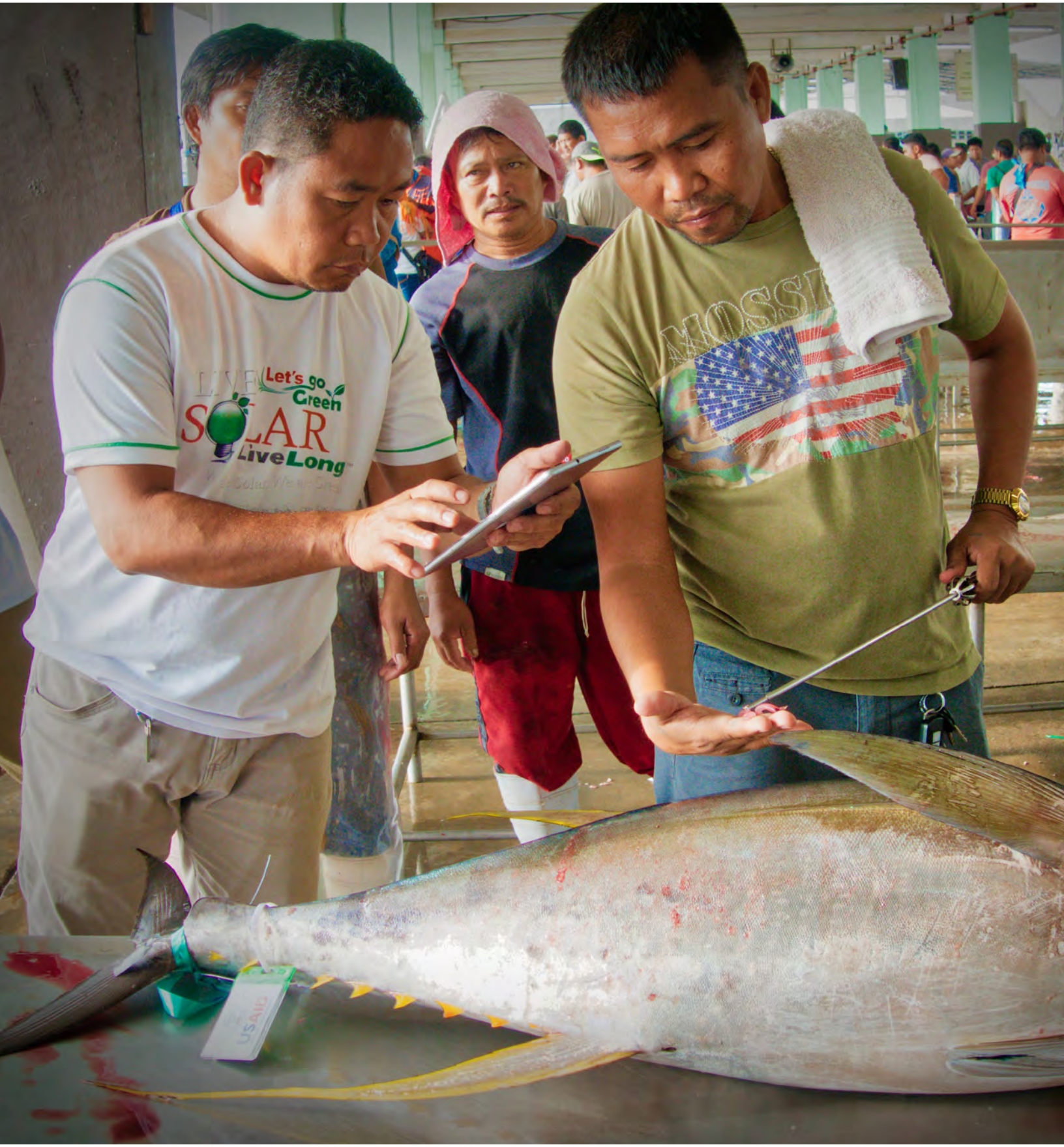
- Hay costos asociados con la recuperación de datos, incluyendo el tiempo del personal y la posible compra de nuevos equipos. Los datos también pueden considerarse un elemento de valor.
- Un incidente que afecte el negocio o los datos puede ocurrir dentro del sistema empresarial, en un sistema de terceros o mientras los datos están en tránsito. Es posible que los datos en los sistemas de proveedores externos no estén cubiertos por una póliza estándar.
- A menudo, las partes extranjeras originan ataques. Esto puede incluir grupos patrocinados por el gobierno o deshonestos con el objetivo de causar un caos y una interrupción general, no necesariamente para dañar una empresa en particular. Las empresas deben entender cuáles incidentes, incluyendo los "desastres naturales", están cubiertos y no cubiertos por la póliza.
- Los ataques pueden afectar la reputación de una empresa e implicar responsabilidad legal. Es posible que se necesiten servicios legales, de TI y otros servicios profesionales para manejar las consecuencias. Las empresas deben aclarar y comprender las responsabilidades potenciales por el pago de multas e indemnizaciones y cualquier otra obligación que surja en caso de un incidente cibernético.
- Cuando los datos personales se ven comprometidos, las leyes pueden exigir que la empresa proporcione una notificación inmediata a las personas y empresas afectadas, además del reembolso del dinero perdido y los costos incurridos, además de otra restitución. Las organizaciones deben verificar si estos requisitos están cubiertos por la política.
- Las compañías de seguros tienen pautas diferentes sobre ransomware u otros pagos de extorsión. Las organizaciones deben comprender de antemano la política y los procedimientos requeridos, de manera especial qué hacer y qué no hacer en estos casos. Las compañías de seguros pueden definir de diferentes maneras los términos relacionados con la ciberseguridad. Las empresas deben comprender lo que cada empresa quiere decir con los términos que utiliza.
- Hay elementos o riesgos que los seguros cibernéticos no cubrirán, como posibles pérdidas futuras o el costo de mejorar los sistemas de seguridad. Una organización debe tener en cuenta que estos gastos deben cubrirse en caso de incidente.

Tomando en cuenta estos puntos, las empresas deben revisar si el seguro de ciberseguridad es apropiado para ellas. Si es así, el plan de recuperación comercial debe incluir los pasos para recopilar la información requerida para presentar un reclamo bajo la póliza de seguro cibernético seleccionada.

15. Considerar contratar a un profesional de TI

Los pasos de esta guía pueden ayudar a una empresa a desarrollar un plan sólido de ciberseguridad y ayudarla a navegar en el crecimiento, los ajustes y la adopción de nuevas tecnologías. En algún momento, puede ser necesario contratar a un profesional de TI para la empresa, ya sea como consultor o como empleado. En tal caso, los propietarios de pequeñas empresas y su personal pueden obtener una comprensión fundamental de la seguridad cibernética a través de esta guía, lo que les permite elegir el tipo de asistencia que sería más valiosa para la empresa.

Lo más importante es conocer los riesgos para la empresa, qué se puede hacer para reducir el riesgo inmediato y cómo planificar para alcanzar los objetivos de reducción de riesgos dentro de las limitaciones de la empresa. Para reiterar, el cibernético es otro riesgo operativo que puede tener consecuencias importantes para una empresa y sus clientes. La conciencia de ciberseguridad puede poner a una empresa en el camino para mejorar. La transformación no tiene por qué ocurrir de la noche a la mañana. Se puede planificar para que las metas incrementales se cumplan de manera periódica con el tiempo. Lo importante es establecer una cultura empresarial que incluya la conciencia de ciberseguridad, saber qué está haciendo la empresa actualmente para abordar el riesgo cibernético y qué se debe hacer para mejorar la ciberseguridad de la organización.



© MELINDA DONNELLY FOR USAID/OCEANS

SI OCURRE UN INCIDENTE DE CIBERSEGURIDAD

Una empresa siempre debe responder con rapidez en caso de un ataque cibernético u otro incidente de ciberseguridad. Una reacción rápida puede ser la diferencia entre un daño menor o una interrupción importante del negocio. Primero, un administrador debe notificar a las personas adecuadas. Esto podría incluir personal interno con roles específicos y consultores externos identificados que pueden realizar servicios especializados que pudiesen ser necesarios, como asegurar operaciones, detener una violación de datos, realizar análisis forense de TI, corregir vulnerabilidades, elaborar memorandos legales para reportes y comunicaciones a las autoridades correspondientes y partes interesadas, como clientes y proveedores. Deben determinar las obligaciones legales necesarias en función del tipo de incidente. Los gobiernos o entidades gubernamentales pueden regular la notificación de infracciones de seguridad de manera diferente, lo que es particularmente cierto cuando se trata de datos personales.

Reanudar Operaciones

En un evento cibernético, puede ser necesario desconectar computadoras y equipos de red para evitar un mayor acceso a los sistemas empresariales y evitar la propagación de malware a equipos no infectados.

Las empresas deben seguir los consejos del profesional de TI de la empresa o del proveedor de antivirus y/o copia de seguridad. Las copias de seguridad completas del sistema, como se mencionó anteriormente, son a menudo la forma más fácil y limpia de restaurar los sistemas a su estado anterior, no afectado, y de reanudar las operaciones. Las organizaciones deben asegurarse de identificar la fuente del ataque para que la misma vulnerabilidad no se vuelva a explotar, dando como resultado otro compromiso de los sistemas empresariales.

Los pasos exactos para restaurar las operaciones dependen de la naturaleza del incidente, la empresa y la información involucrada.

Gestionar las Comunicaciones de forma efectiva

Después de que una empresa haya sido objeto de un ciberataque, la estrategia de comunicación debe cambiar al modo de emergencia. Lo que se dice de manera pública en el momento es fundamental para sobrevivir a un ataque, mantener la confianza y la reputación empresarial, y minimizar la responsabilidad legal. El Instituto de Ingeniería de Software de la Universidad Carnegie Mellon ha desarrollado una Guía para Comunicación Efectiva de Gestión de Incidentes[29], que establece cómo abordar las comunicaciones

CUANDO OCURRE UN CIBERATAQUE

Los admin deben tener una lista impresa de contactos de emergencia si se presentan incidentes de ciberseguridad. Deben asegurarse de que estos contactos no dependan del correo electrónico de la empresa o de la funcionalidad del servicio telefónico. Además, el admin debe revisar que cada persona conozca sus responsabilidades en caso de un incidente cibernético.

Si corresponde, el administrador puede comunicarse con el procesador de pagos de la empresa y recopilar cualquier información que pueda ser necesaria para la recuperación de incidentes.

PREPARACIÓN PARA UN CIBERATAQUE

Las organizaciones pueden simular un incidente cibernético para probar el tiempo de respuesta de la empresa y si cada empleado conoce su función. Utilice copias de seguridad para practicar reanudación de operaciones.

29 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651816

INSTITUTO NACIONAL DE NORMAS Y TECNOLOGÍA

El NIST elabora normas de ciberseguridad, directrices, mejores prácticas y otros recursos. Es un gran recurso tanto para las grandes como para las pequeñas empresas.

- Rincón de la ciberseguridad para pequeñas empresas
- Guía de inicio rápido del marco de ciberseguridad
- Guías de ciberseguridad de uso general
- Guía de respuesta a un incidente cibernético

durante un incidente. Esa guía también hace referencia a las comunicaciones al Marco de Seguridad Cibernética (CSF, por sus siglas en inglés) del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), lo que facilita su integración en otros esfuerzos de comunicación.

Las empresas deben desarrollar un plan de comunicaciones siguiendo la guía y las diez consideraciones principales de Carnegie Mellon para una Comunicación Efectiva de Gestión de Incidentes.[30] Las organizaciones deben:

1. Considerar la comunicación como una iniciativa estratégica.
2. Tener un plan de comunicación reactivo en marcha.
3. Considerar los mensajes de la empresa, la reputación y las partes interesadas como factores críticos en el desarrollo de planes de comunicación.
4. En el plan de comunicación, definir y determinar claramente los siguientes componentes clave:
   - Establecer el propósito;
   - Determinar la audiencia;
   - Definir roles y responsabilidades;
   - Comprender y estandarizar los mensajes;
   - Determinar y establecer canales de comunicación; y
   - Determinar los métodos de distribución de mensajes.
5. Capacitar y probar de manera continua el plan. Asegúrese de que el plan funcione y, así como el plan de respuesta a incidentes, pruébelo antes para que esté listo para la gestión de incidentes.

Compartir información y comunicarse con el público y/o los clientes es apropiado en la mayoría de los escenarios, pero es importante que las empresas se comuniquen con la policía local y otras autoridades relevantes antes de hacer anuncios públicos. El método y el contenido de la comunicación varían según el escenario. También se debe considerar la gestión de medios porque los medios de comunicación podrían informar el incidente, por lo que es importante comprender los incentivos de los medios y los de la empresa, además de la alineación de los dos.

NOTIFICAR A LAS AUTORIDADES

Cuando ocurren delitos relacionados con Internet, por ejemplo, hackeos, ransomware, etc., actuar de forma rápida puede ayudar a minimizar el daño a la empresa y limitar la responsabilidad legal si hay problemas de cumplimiento. Cada jurisdicción tiene requisitos de reportes y plazos específicos, por lo que las empresas deben consultar con las autoridades locales antes de que ocurra un incidente para saber qué requisitos aplican a la empresa. Esto incluye requisitos legales específicos y recomendaciones sobre cuándo involucrar a las autoridades si hubiesen amenazas o demandas de rescate. Los delitos cibernéticos pueden investigarse y procesarse de manera diferente a otros delitos, por lo que las organizaciones deben notificar a todas las autoridades correspondientes que

supervisarían el incidente. Es mejor conocer esta información con anticipación para que el personal clave conozca los requisitos para presentar reportes.

En general, las empresas deben esperar proporcionar información precisa y completa sobre el ataque y las partes involucradas, lo que incluye:

- El tipo de incidente, cuándo se detectó y qué sucedió.
- Si hubo transacciones financieras involucradas, como un rescate. Es probable que las agencias gubernamentales requieran los números y nombres de los titulares de las cuentas, las fechas y montos de las transacciones, los destinos de las transacciones, etc.
- Copias de las comunicaciones entre el atacante y la víctima.
- Cualquier otra información que pueda ser relevante para el hackeo reportado, incluyendo nombre e información de contacto de las empresas y las personas afectadas por la exposición de sus datos.

Los administradores deben ser conscientes de que los atacantes utilizan técnicas que les permiten penetrar y permanecer en una red sin ser detectados hasta que lanzan un ataque. Por lo tanto, puede haber un lapso de tiempo entre la infracción inicial y las actividades ilegales que se llevan a cabo. Por ejemplo, se puede violar el acceso a los datos comerciales más críticos de una red, pero es posible que la empresa no se entere hasta más tarde, cuando los clientes llamen para reportar cargos no autorizados en sus tarjetas de crédito. Las organizaciones deben asegurarse de documentar todas las circunstancias y sus plazos para obtener un registro completo del incidente. Esto podría incluir inicios de sesión en la red, registros de tráfico, direcciones de Protocolo de Internet (IP, por sus siglas en inglés), sitios web involucrados, órdenes electrónicas para realizar transferencias, etc. Un profesional de TI puede ayudar a recopilar toda esta información. En caso de duda, las empresas deben agregar la información al registro de incidentes. La información que en apariencia no tiene importancia podría ser crucial, especialmente cuando se consideran todas las circunstancias. Si se contrata a un profesional de TI, también debe verificar que el atacante ya no esté presente en la red. El profesional de TI debe actuar de enlace con las autoridades con respecto a la investigación del incidente y la conservación de la evidencia.

NOTIFICAR A LOS PROVEEDORES DE SERVICIOS

Los ataques recientes han seguido un modelo de "hub-and-spoke", ya que los atacantes violan los sistemas desarrollados por los proveedores para atacar a sus clientes. Si el incidente involucra a proveedores de servicios, como el procesador de pagos comerciales, para realizar pagos no autorizados o la instalación de un proveedor donde se almacenan datos, las empresas deben reportarlos y trabajar juntos en consulta con las autoridades para mitigar el daño y acelerar la recuperación. De igual manera, una empresa podría ser parte de las cadenas de suministro y el incidente cibernético podría haber expuesto la cadena en su totalidad o en parte. Las organizaciones deben notificar a los socios inferiores y superiores sobre el incidente, y deben compartir la información relevante.

30 https://insights.sei.cmu.edu/blog/top-10-considerations-for-effective-incident-management-communications/

CREAR COMUNICACIONES PROACTIVAS

Las empresas deben redactar la plantilla del mensaje inicial a los consumidores/clientes y proveedores en caso de un ataque de ciberseguridad que exponga sus datos. Deben adaptar este mensaje a los tipos de datos de clientes y proveedores recopilados y almacenados en la empresa y garantizar que cumpla con los requisitos legales aplicables.

HAGA COPIAS IMPRESAS

Usando la información compilada después esta guía, las organizaciones deben preparar una carpeta de emergencia de seguridad cibernética que contenga copias impresas de todos los documentos preparados para la mitigación y eventualidades cibernéticas. Deben asegurarse de que se pueda acceder a la carpeta si los sistemas informáticos no se pueden utilizar en caso de un incidente cibernético.

Los administradores deben discutir estos planes con los proveedores de servicios y proveedores como parte de la preparación antes de un ataque para que todos conozcan el proceso para reportar un incidente, la información necesaria para obtener soporte y cómo restaurar las operaciones. Es necesario documentar ese proceso como parte de la estrategia de ciberseguridad de la empresa.

NOTIFICAR A LOS CLIENTES

La divulgación oportuna y sincera, además de seguir el asesoramiento de expertos y coordinarse con las autoridades, puede ayudar a asegurar a todos los afectados que sus intereses están siendo protegidos y que los impactos inmediatos y a largo plazo del incidente se están minimizando.

Las notificaciones generalmente deben cumplir con los requisitos legales o reglamentarios. Al notificar por primera vez a las autoridades, las empresas deben preguntarse si las leyes o reglamentos exigen una forma específica de notificar a las partes afectadas, las características de esas notificaciones y el plazo para hacerlo. Es importante que las interacciones no comprometan las investigaciones de las autoridades, por lo que su participación en el momento y el contenido de las comunicaciones de la organización es crucial.

Las empresas deben considerar incluir la siguiente información al desarrollar comunicaciones:

- Una explicación simple y veraz del incidente;
- Una explicación de los datos que se vieron comprometidos y cómo la violación puede afectar a los clientes y proveedores ahora y en el futuro previsible;
- Referencia a leyes o reglamentos aplicables y agencias involucradas en el caso;
- Qué acciones se están tomando para recuperarse del incidente y para proteger los intereses de los clientes y proveedores;
- Asesoramiento sobre lo que los clientes y proveedores pueden hacer para protegerse si sus datos se han visto comprometidos o se han utilizado de manera indebida;
- Un punto de contacto de la empresa para responder preguntas;
- Medios por los cuales los clientes y proveedores se mantendrán informados de los desarrollos (por ejemplo, vía correo electrónico, en el sitio web de la empresa, etc.), siguiendo los requisitos legales aplicables.

REDES SOCIALES

Las organizaciones deben asumir que el incidente se compartirá en las redes sociales. El plan de comunicaciones debe incluir un componente sobre cómo utilizar las redes sociales de manera efectiva. Los mismos puntos descritos anteriormente se aplican a las comunicaciones en los medios sociales, pero es probable que todo lo que se publique en las redes sociales se haga público, más allá del grupo de clientes o proveedores afectados.

Aprendiendo del Incidente

Una vez que se restablecen las operaciones normales, las empresas deben hacer un balance de lo que sucedió, a qué pudieron acceder los atacantes y qué tan efectivo funcionó el plan de respuesta. Luego, las organizaciones pueden revisar las medidas de seguridad implementadas y buscar métodos para fortalecerlas para ayudar a evitar que vuelva a ocurrir un ataque similar, así como cualquier otro tipo de ataques para los que la empresa no esté preparada. (Consulte "Categorías de Amenazas", en la Parte I de esta guía). Deben considerar si hay algo que se pueda hacer en el futuro para mejorar una respuesta, pensando en cómo se descubrió la infracción, cómo se comunicó de manera interna y externa, y cómo se resolvió. También podría ser más fácil planificar incidentes futuros con un conocimiento más preciso de los costos (financieros, de reputación y operativos, entre otros) de un ataque a la empresa y qué medidas valen la pena para ayudar a prevenirlo.

CAPTURA DE APRENDIZAJE

Después de cada incidente y al menos una vez al año, las organizaciones deben actualizar y desarrollar aún más el plan de respuesta empresarial y la capacitación del personal para documentar lo que se ha aprendido y los cambios a implementar.

CONCLUSIÓN

Los pasos descritos en esta guía por lo general no requieren un alto nivel de experiencia o un gran gasto de fondos, pero sí necesitan reflexión y planificación para ponerlos en práctica. Si bien estas son acciones básicas y de bajo costo que una pequeña empresa puede implementar, los pasos se pueden integrar con estrategias más sofisticadas a medida que la organización madura en su comprensión de cuestiones cibernéticas y a medida que la empresa crece. Conforme la tecnología cibernética se desarrolle y evolucione, surgirán nuevas amenazas y se tendrán disponibles nuevos recursos para las empresas. Mientras tanto, los aspectos cubiertos en esta guía brindan un enfoque básico sólido y un plan para desarrollar ciberseguridad y resiliencia en una pequeña empresa.

USAID
FROM THE AMERICAN PEOPLE